El camino hacia un ciberespacio estable y seguro

Vega Buono Sofía[3]

La complejidad del ciberespacio radica más en los problemas conceptuales y en los intereses nacionales de cada Estado que en su propia naturaleza. Ciertamente, la comprensión convencional de la Defensa y la disuasión ha sido alterada por la revolución tecnológica y cibernética desarrollada a lo largo de las últimas décadas. Ello supone un peligro de alto voltaje para la Seguridad Nacional y la paz mundial, puesto que la proliferación de las capacidades cibernéticas ofensivas y las armas digitales están superando ampliamente el diseño de marcos conceptuales para interpretar y abordar nuevas realidades.

El dominio rebelde

No existe consenso sobre las acciones y estrategias cibernéticas maliciosas ni sobre qué debe hacerse al respecto. Los mecanismos de seguridad convencionales, sin mencionar la obsolescencia de los principios del delito cibernético, no pueden aplicarse ante ciberataques o explotaciones cibernéticas. En rigor, las nociones tradicionales de la guerra presentan serios problemas a la hora de conceptualizarlos, ya que exceden la lógica clausewitziana de una guerra intrínsecamente violenta, saturada por los daños colaterales, la pérdida de vidas significativas y los profundos niveles de destrucción física. Por su parte, los las actividades cibernéticas no provocan lesiones físicas ni son inherentemente violentos; en su mayoría, son ejecutadas por actores no estatales – no son considerados sujetos del Derecho Internacional -, capaces de mantenerse en el anonimato; no precisan ejércitos regulares ni algún otro tipo de fuerza armada: su arsenal es digital (infiltración a sistemas informáticos, ransomware, malware, etc.) y sus efectos son indirectos – daños sociales, económicos, financieros, políticos -; a menos que no sean agresiones localizadas, la distinción entre objetivos militares y civiles se disuelve, pues los sistemas informáticos forman parte de la vida cotidiana de la sociedad en su conjunto, extendiendo sus efectos indiscriminadamente (Kello, 2013).

Asimismo, las actividades cibernéticas maliciosas rompen con el eje de la teoría clásica de Seguridad, que presupone que el éxito de la política de Seguridad yace en ser capaces de mantener al adversario fuera del territorio nacional. Aquí, el enemigo ya se encuentra infiltrado en los sistemas vitales de su objetivo, sin que el mismo sea consciente de ello. En promedio, las compañías tardan 230 días en detectar intrusiones cibernéticas en sus sistemas informáticos. Goldman y Harknett (2016) sostienen que, en cuanto al ciberespacio, la defensa prevalece en contacto permanente con el enemigo. Las acciones cibernéticas no son actos clásicos de guerra. No obstante, no corresponden a actos clásicos de paz tampoco. Por tanto, ¿qué son? Kello (2017) plantea que ninguna operación cibernética, incluso hasta las más severas, se ajusta al binomio guerra-paz, ampliando la brecha entre ambas nociones e incorporando una tercera situación intermedia - a la cual denomina “un-peace”- que comprende aquellas acciones de criterio medio tales como el ciberdelito, la explotación cibernética o los ciberataques.

¿Cómo reglamentar sobre algo abstracto?

Si bien los Estados son conscientes de la relevancia del quinto dominio, pues existen numerosos programas de políticas públicas en materia ciberespacial en varios Estados, ello no se traduce en acciones precisas dentro de la comunidad internacional para sentar las bases conceptuales del proceso de elaboración de cyber norms. La anomia cibernética en el Sistema Internacional permite tantas interpretaciones de la ciberseguridad como países en el mundo. En este sentido, tanto la Federación de Rusia, así como la República Popular China destinan sus políticas de ciberseguridad al control de la información dentro de sus jurisdicciones internas, protegiendo los secretos de Estado y otras informaciones que, de ser difundidas, pueden poner en peligro al régimen político, mientras que, por ejemplo, los países europeos orientan sus políticas de seguridad cibernética hacia la protección de sus infraestructuras críticas. Sin dudas, dicha controversia conceptual entre oriente y occidente obstruye el consenso internacional respecto al significado de la ciberseguridad, ergo, normativa.

El inexistente consenso sobre las normas y principios de comportamiento de los Estados en el ciberespacio conduce a la falta de reglamentación del mismo y de un marco legal de respuesta, lo cual lo convierte en un dominio de conflicto y competencia, amenazando la estabilidad de la Seguridad Internacional permanentemente. A lo largo de los años,

3 Estudiante avanzada de la Licenciatura en Relaciones Internacionales (Universidad Nacional de Lanús)

los esfuerzos de la comunidad internacional para desarrollar normas cibernéticas han fracasado sistemáticamente. El Manual de Tallin, elaborado por expertos de la OTAN en 2013, ha intentado ajustar tales cuestiones, pero solo ha logrado confundir y empañar el panorama. El Grupo de Expertos Gubernamentales (GGE) y el Grupo de Trabajo de Composición Abierta (OEWG) de Naciones Unidas celebra sesiones periódicamente, pero no hay avances sustantivos ni se vaticina un acuerdo general respecto a la regulación del ciberespacio. En 2017, luego de que los Estados miembros del GGE no pudieron acordar si el Derecho Internacional humanitario debería aplicarse para el espacio cibernético, fracasó una de las últimas iniciativas para pautar normas sólidas desde el seno de las Naciones Unidas.

Desde el año 2016, las discusiones internacionales sobre cyber norms y la ciber disuasión se han descuidado deliberadamente, pues los Estados participantes y beneficiarios de la guerra cibernética no tienen la intención de impulsar iniciativas o promover propuestas sobre las normas cibernéticas porque perder un dominio indefinido, sin reglas de juego, poco costoso y sin sanciones o represalias no les es funcional a sus intereses nacionales. Desde luego, la escalada en las tensiones geopolíticas entre las principales potencias cibernéticas y el alto grado de militarización del ciberespacio no construyen un escenario propicio para que los Estados concilien un conjunto de normas que restrinjan al máximo posible las operaciones cibernéticas.

Con la crisis viene la oportunidad

Pese a ello, la pandemia del coronavirus ha alzado nuevas voces y fortalecido otras que abogan por una mayor atención y preocupación sobre el quinto dominio. El 5 de mayo del corriente año, las agencias nacionales de ciberseguridad de los Estados Unidos y Reino Unido advirtieron que no sólo los piratas informáticos están explotando las vulnerabilidades cibernéticas expuestas tras la pandemia de coronavirus, sino también ciberdelincuentes que trabajaban en nombre de los Estados nacionales. En rigor, las investigaciones relacionadas al COVID-19 se enfrentan a amenazas cibernéticas reales, al mismo tiempo que forman parte del campo de batalla de pujas por el poder y el liderazgo mundial. Los actores maliciosos promovidos por los Estados intentan obtener datos específicos de propiedad intelectual y salud pública respecto a tratamientos, vacunas, pruebas de redes y personal involucrado en la investigación. Los ciberataques en las instituciones de salud o en agencias gubernamentales ponen en riesgo la consecución de tratamientos seguros y efectivos, ya que se busca socavar la capacidad de respuesta del otro Estado frente a la crisis sanitaria.

Ciertos países de Europa han manifestado su preocupación por el impacto que puede llegar a ocasionar la ola de ataques cibernéticos en curso. Verbigracia, Países Bajos afirma que estos tipos de acciones cibernéticas constituyen violaciones del Derecho Internacional. En concordancia, la República Checa, que ha sufrido un grave ataque en el Hospital Universitario de Brno, institución clave en la lucha contra el coronavirus, enfatizó la urgencia de una acción global coordinada en disposición de proteger de los ciberataques, ciberdelitos o explotación cibernética a los sectores prioritarios durante la presente crisis. Estonia, uno de los Estados más digitalizados de la Unión Europea y punta de lanza en la ciberseguridad, ratifica la responsabilidad de la comunidad internacional de edificar un ciberespacio seguro y más funcional que nunca porque lo que está en juego es la seguridad de los hospitales y servicios médicos esenciales, nada más ni nada menos. La UE continúa reforzando su compromiso con un ciberespacio estable, pacífico y seguro, fortaleciendo la cooperación internacional para promover el orden normativo en este ámbito. Ciertamente, contra todo pronóstico, la Secretaría del OEWG se encuentra confeccionando un informe final que expone y examina las normas, el Derecho Internacional, el desarrollo de capacidades y otras medidas propuestas para garantizar la estabilidad del ciberespacio.

¿Qué es la pandemia si no la voz de la conciencia sobre la importancia del ciberespacio? Si el incremento de las ciber amenazas y de ciberdelitos durante una pandemia no fomenta el consenso sobre las normas cibernéticas y la acción global sobre cuestiones de ciberseguridad, entonces ¿qué tendrá que suceder para que ocurra?

Bibliografía

Gold, J. (2020). Amid COVID-Related Cyber Threats, the Netherlands Leads UN Efforts. Council of Foreign Relations. Disponible en https://www.cfr.org/blog/amid-covid-related-cyber-threats-netherlands-leads-un-efforts

Van der Meer, S. (2020). Could the Coronavirus Crisis Strengthen Due Diligence in Cyberspace? Council of Foreign Relations. Disponible en https://www.cfr.org/blog/could-coronavirus-crisis-strengthen-due-diligence-cyberspace

Goldman, E. y Harknett, R. (2016). The Search for Cyber Fundamentals. Journal of Information Warfare Vol. 15, No. 2, pp. 81-88. Disponible en https://www.jstor.org/stable/26487534

Kello, Lucas (2013). The Meaning of the Cyber Revolution. Perils to Theory and Statecraft. International Security, Vol. 38, No. 2, pp. 7–40. Disponible en https://www.mitpressjournals.org/doi/pdfplus/10.1162/ISEC_a_00138

Kello, Lucas (2017). The Virtual Weapon and International Order. Yale University Press.

Meyer, Paul (2018). Global Cyber Security Norms: A Proliferation Problem? ITC for Peace Foundation. Disponible en https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2018-Global-Cyber-Security-Norms.pdf